# Cómo usar los teléfonos inteligentes con inteligencia:

## *Consejos para los consumidores*

Hoja 15A informativa para el consumidor • Mayo de 2013

Nuestros teléfonos se han convertido en computadoras de bolsillo. Piense en la información almacenada en su teléfono inteligente: registros de llamada, mensajes de texto, su ubicación, sus contactos, fotos, videos y su historial de navegación por la web. Piense en todo lo que pueden hacer: pasar películas a demanda, llamar un taxi, hacer compras y hablarle, entre otras cosas.

Si usted dice, como muchos otros norteamericanos, que su vida está en su teléfono, ha llegado la hora de usarlo en forma inteligente. Su seguridad depende de ello.

### Riesgos de los teléfonos inteligentes: tome conciencia

Los teléfonos inteligentes (junto con las tabletas y otros dispositivos portátiles que pueden acceder a Internet) crean riesgos de privacidad, de la misma manera que sus contrapartes de escritorio. Pueden ser blanco de *malware y spyware* (virus) y vulnerables a la acción de *hackers* (piratas). Aun así, muchos consumidores no protegen sus teléfonos con software de seguridad, y ni siquiera con un código de ingreso.

Los teléfonos inteligentes almacenan información muy personal que queremos mantener privada, como mensajes de texto, fotos y la información de contacto de nuestros amigos. Si usa su teléfono para operaciones bancarias en línea, la contraseña de su cuenta puede ser almacenada en el teléfono. Y algunas de las aplicaciones que hacen que sus teléfonos sean tan útiles pueden capturar una gran cantidad de información personal.

### Privacidad en los teléfonos inteligentes: es suya

Su privacidad puede correr riesgo aun si tiene el teléfono consigo en todo momento. No sea complaciente y tome los pasos necesarios para protegerse hoy mismo. Vea los consejos que le damos a continuación y después vaya a la sección *Para obtener más información* al final de esta hoja informativa para ver recursos adicionales.

### ☑ Primero, cuide de su seguridad personal

Manténgase alerta al usar su teléfono en lugares públicos: los teléfonos inteligentes son valiosos. Los delincuentes arrebatan teléfonos de personas distraídas que están hablando o enviando mensajes de texto, con frecuencia lesionándolas. Los teléfonos inteligentes robados no solo tienen valor en el mercado de reventa, sino que también son valiosos para los ladrones



Office of the Attorney General
California Department of Justice

Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

de identidad, que usan su información personal almacenada para cometer delitos.

Cuando maneje, apague su teléfono. Si tiene que hacer una llamada o enviar un mensaje, pare al costado del camino. Si apaga su teléfono inteligente cuando está detrás del volante, podrá salvar vidas, incluso la suya.

## ☑ Cuide de la seguridad de su teléfono

- Sepa dónde está su teléfono en todo momento. No deje que un desconocido tenga acceso al mismo; el *malware, spyware* o las aplicaciones de rastreo se pueden instalar en muy pocos minutos.
- Proteja su teléfono con una contraseña o código.
- Instale software de seguridad. Verifique que esté siempre actualizado.
- Mantenga al día el sistema operativo de su teléfono. De esa manera lo protegerá con parches para solucionar errores o *hacks*.
- Use una *app* o servicio que le permita borrar en forma remota la información del teléfono en caso de que lo haya perdido o se lo hayan robado. Tiene que configurar esta opción por adelantado, antes de que su teléfono desaparezca.
- Haga una copia de reserva del contenido de su teléfono en su computadora o un sistema de almacenamiento para teléfonos móviles en la nube. Los fabricantes de estos dispositivos y otros ofrecen sistemas de almacenamiento móvil en la nube.
- También puede proteger mejor su información privada usando las configuraciones de su teléfono inteligente.
- Autobloqueo: Los teléfonos son pequeños y se pueden perder fácilmente. Configure su teléfono para que se autobloquee en cinco minutos y haya que ingresar una contraseña para desbloquearlo.
- Servicios de ubicación: Su teléfono puede rastrear su ubicación por muchas razones útiles: darle instrucciones para llegar a un lugar, brindarle actualizaciones de tráfico, encontrar el restaurante más cercano, darle informes meteorológicos. Usted puede permitir que el teléfono acceda a su ubicación cuando quiera, pero no tiene que hacerlo siempre.
  - En un teléfono Android, vaya a *Settings*, después *Location*, y desactive la casilla. Después podrá decidir si quiere activar los servicios de ubicación cuando la *app* le pida acceso.
  - En un iPhone u otro dispositivo iOS, vaya a *Location Services* bajo *Privacy* en *Settings*. Puede desactivar el servicio. También puede elegir qué funciones y *apps* tendrán acceso a su ubicación,
  - En un teléfono Windows, puede desactivar todo el acceso de *apps* a información sobre su ubicación y su recolección por medio del servicio de ubicación de Windows Phone. Vaya a *Settings*, después *Location*, y coloque la llave en la posición *Off*.
  - En un BlackBerry 10, seleccione el icono *Settings* en la pantalla principal, después elija *Location Services* de la lista, y use el botón *Location Services* para encender o apagar los servicios de ubicación.
  - En un BlackBerry 7 o anterior, seleccione *Options* en la pantalla principal, después *Device,* y después *Location Settings*. Use el botón para encender o apagar los servicios de ubicación y la asistencia por GPS.

## ☑ Verifique su red

- Tenga cuidado cuando pague por teléfono al comprar su latte. Las redes WiFi públicas gratuitas generalmente no son seguras, y los ladrones de información lo saben. Se sientan en cafés, centros comerciales y otros

lugares públicos y observan cómo usted usa la Internet. Sus contraseñas, números de cuenta y fotografías pueden caer en su poder. Cuando use WiFi públicos, no realice transacciones que puedan revelar sus datos personales o contraseñas.

### ☑ Verifique las apps

Hay más de un millón de *apps* móviles disponibles en la actualidad. Nos permiten realizar cosas maravillosas y útiles. También pueden acceder a nuestra información personal e incluso las funciones del teléfono. Haga una pausa y verifique las características de la última *app* de moda antes de descargarla.

- En la plataforma/tienda de la *app*, consulte su política de privacidad. Lea la política para ver qué dice sobre la información personal recolectada, y cómo la usan y comparten. Si ve algo que no le gusta, no descargue esa *app*.
- En teléfonos Android, la pestaña *Permissions* en las páginas de *apps* de la tienda GooglePlay muestra información y describe las funciones que la *app* puede acceder en su teléfono. Por ejemplo, puede mostrar que una app puede hacer llamadas telefónicas e incurrir en cargos. Si no le gusta los permisos que tiene que dar, no descargue la *app*.
- Una vez que haya descargado la *app*, preste atención a cualquier aviso que le pida permiso para acceder a su ubicación u otra información.
- Una vez que haya descargado la *app*, busque en la misma su política de privacidad y una manera de configurar la misma. Quizás pueda elegir qué información puede recolectar la *app* y cómo la usa.
- Las leyes de California requieren que las *apps* tengan una política de privacidad.[1] Si no puede encontrar la política de privacidad de la *app* en la plataforma/tienda o dentro de la *app* misma, o si tiene una queja sobre las prácticas de privacidad de la *app*, repórtela.
  - Para *apps* en la tienda de Microsoft Windows: Busque un enlace marcado *"Report app to Microsoft"* o *"Report concern to Microsoft"*.
  - Para *apps* en el AppStore de Apple: *Visite www.apple.com/privacy/contact/*.
  - Para *apps* en GooglePlay: Busque *"Flag as inappropriate"* en la página de descripción de la *app* o visite *https://support.google.com/googleplay/android-developer/contact/takedown*.
  - Para *apps* en BlackBerry World: Envíe correo electrónico a *privacyoffice@rimcom*.
  - Denuncia al Procurador General de California: *www.oag.ca.gov/contact/consumer -complaint-against-business-or-company*

## Para obtener más información

Análisis de *apps,* Common Sense Media, disponible en *www.commonsensemedia.org/app-reviews*

"How to clear your data off a device", (*Cómo borrar los datos de un dispositivo*), Computerworld (Agosto de 2012), disponible en *http://www.computerworld.com/s/article/9229969/How_to_clear_your_data_off_a_device*

"Before It's Gone: Steps to Deter Smartphone Thefts & Protect Personal Info", (*Antes de perderlo: pasos para desalentar el robo de teléfonos inteligentes y proteger su información personal*), CTIA (The Wireless Association), disponible en www.ctia.org/consumer_info/index.cfm/AID/12084.

"The Best Mobile Security Apps", (*Las mejores apps de seguridad para dispositivos móviles*), PC Magazine (Mayo de 2012), disponible en *www.pcmag.com/article2/0,2817,2402099,00.asp*

"How to Remotely Disable Your Lost or Stolen Phone", (*Cómo desactivar en forma remota su teléfono perdido o robado*), PC Magazine (Abril de 2012), disponible en h*ttp://www.pcmag.com/article2/0,2817,2352755,00.asp.*



NOTAS

[1] Ley de Protección de la Privacidad en Línea de California, Código Comercial y Profesional, §§ 22575-22579.